Cybersecurity: From Months to Milliseconds

Peter Fonash and Phyllis Schneck, US Department of Homeland Security

Computer technology is the nexus of our critical infrastructures, yet it remains extremely vulnerable to cyberattacks. A proposed Integrated Adaptive Cyber Defense architecture promises to create a healthy cyber ecosystem by automating many risk decisions and optimizing human oversight of security processes too complex or important for machines alone to solve.

Great efficiencies have been achieved with the integration of computers into our daily lives. Advances in information and communications technology (ICT) enable us to automate business processes, manage critical infrastructures, and establish pervasive connectivity among users and systems. This technology has become so inexpensive that we are moving to the next phase of integration, interconnecting a plethora of devices in the Internet of Things (IoT) that will allow full control of embedded systems in homes, vehicles, and public and private infrastructure, resulting in even greater effectiveness and cost savings.[1] The IoT is expanding quickly. As Figure 1 shows, Cisco predicts that it will grow from about 14 billion devices today to more than 50 billion by 2020.[2]

Many "things" in the IoT provide greater convenience or safety. For example, users can remotely activate their home thermostat to warm the house shortly before arrival, check door locks or review surveillance camera footage while away, or receive a reminder from their refrigerator to buy milk on the way home. Embedded automotive systems can monitor and control critical functions such as tire pressure, door openings, proximity to other vehicles, and vehicular health via remote connectivity to the car manufacturer. Medical IoT applications let doctors remotely monitor a patient's heartbeat[3] and patients better self-manage diabetes.[4]

While new and emerging IoT technologies offer many benefits, they can also result in serious harm if not properly protected. For example, a maliciously activated automated insulin injector could lead to death. In fact, cybersecurity firm Cylance has identified more than 300 medical devices vulnerable to remote cyberattack.[5] Likewise, a hacker could remotely take control of a vehicle's automated systems and cause it to crash.

Because of our increasing dependency on computer technology for business, critical infrastructures, communications, and various IoT devices, major cyberattacks

FIGURE 1. The Internet of Things is expected to grow from about 14 million devices to more than 50 billion by 2020. Source: theconnectivist.com.

could cripple our economy, disrupt our infrastructure, and cause loss of life. Accordingly, dramatic cybersecurity improvements are a necessity. While we cannot eliminate every cyber threat, we can manage them by protecting assets more effectively and efficiently according to their value. This approach requires a paradigm shift from how we perform cybersecurity today.

To attain true cybersecurity effectiveness, we must accelerate our detection and response capabilities from people time to machine time—from months to milliseconds. Today, there is almost always a "human in the loop" actively managing the process; although that can help avert unintended consequences, it also means that the attack is often over before preventative action can be taken. This calls for automating many risk decisions and optimizing human oversight of cybersecurity processes too complex or important for machines alone to solve.

CURRENT CYBER LANDSCAPE

Today's cyberattacks are extremely varied and sophisticated. Three key factors contribute to this challenge: the increasing speed at which attackers can successfully attack; the wide range of attackers and attacks to defend against; and the disparate, piecemeal approach implemented in most current cybersecurity solutions.

Time to attack and defend
Of fundamental concern is the long delay between the launch and discovery of cyberattacks, a situation that must improve.

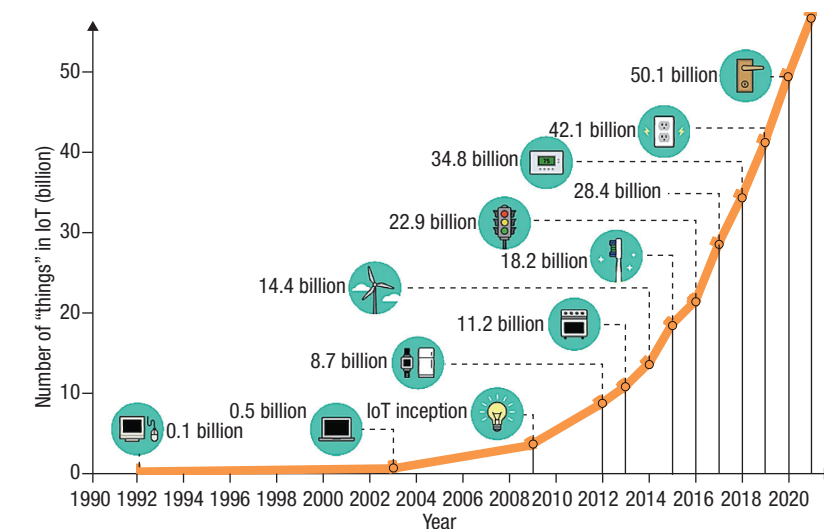Figure 2 compares attacker efficiency, as measured by the time (in days or fractions of days) it takes an attacker to complete a successful infiltration, to defender efficiency, as measured by the time it takes to discover an attack. The solid lines represent a linear regression of the actual data. Over 10 years, attackers successfully improved their efficiency in compromising systems from less than 75 percent successful intrusions occurring within days in 2004 to around 90 percent efficiency in 2013. However, the efficiency to detect attacks within days only improved from about 13 to 20 percent over the same time period. Clearly, then, during the past decade attackers have improved efficiency at a greater rate than defenders. The growing "innovation gap" between the two lines in Figure 2 clearly highlights the need for new approaches to cybersecurity defense.

Breadth of attackers and attacks
Verizon's *2014 Data Breach Investigations Report* (www.verizonenterprise .com/DBIR) states that "2013 may be remembered as the year of the retailer breach, but a comprehensive assessment suggests it was a year of transition from geopolitical attacks to large-scale attacks on payment card systems." Cyberattackers are characterized by their resources and capabilities, intentions and motivations, degree of access, and risk aversion. They include:

› nuisance hackers who use publicly known attacks on unpatched targets of opportunity;
› organized criminals seeking financial gain who use known attacks, slightly alter known attacks to avoid antivirus detection, or develop new attacks;
› sophisticated hackers with a wide variety of intentions and motivations;
› terrorists who seek financial gain to fund their operations or use cyberattacks as a tool to harm their adversaries; and,
› nation-states with varying capabilities, resources, and motivations.

Attackers' intentions drive their target selections. For example, nuisance hackers and organized criminals typically target average citizens and retail companies, while sophisticated hackers, terrorists, and nation-states often attempt to infiltrate foreign government agencies and their contractors as well as companies possessing intellectual property of significant economic value. Well-resourced attackers will often target a large organization's most vulnerable partners as well.
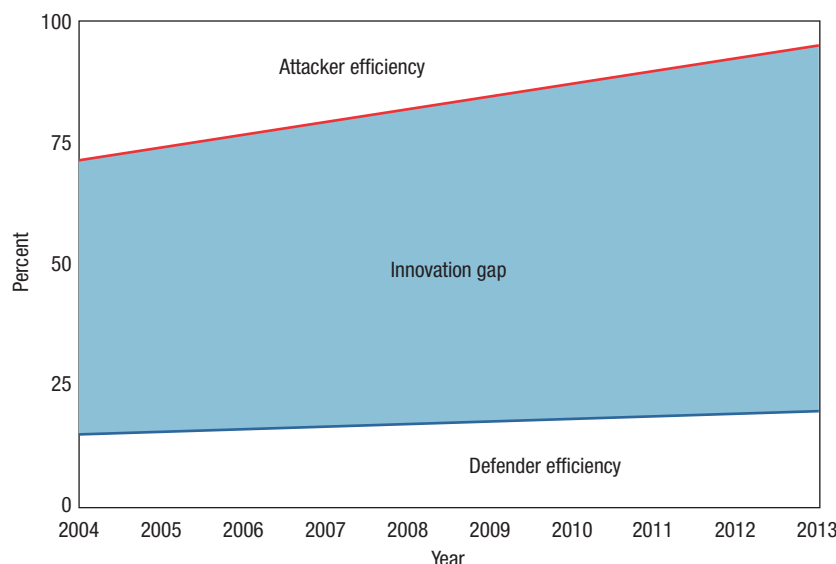
FIGURE 2. Attacker versus defender efficiency. Attackers successfully improved their efficiency in compromising systems in days from less than 75 percent in 2004 to around 90 percent in 2013, but the efficiency to detect attacks within days only improved from about 13 to 20 percent over the same time period. Source: adapted from Verizon's *2014 Data Breach Investigations Report* (www.verizonenterprise.com/DBIR).

Cybersecurity investments

Cybersecurity investments currently follow a piecemeal approach in which disparate proprietary point solutions are linked together uniquely for each enterprise. The situation is akin to the US housing construction market before the 20th century when few building codes existed and each home was custom-built, resulting in higher installation and labor costs, and safety problems such as faulty wiring and vulnerability to severe weather, fire, and earthquakes. We need the equivalent of building codes for cybersecurity and modular, scalable, interchangeable solutions.

However, assessing the appropriate level of cybersecurity investment and correctly integrating available products and services is problematic. This is exacerbated by the constant evolution of technology and attacker tactics. Although organizations have made progress in quantifying the cost benefits of cybersecurity investments, determining whether such investments are commensurate with an organization's risk remains an immature process.

CHARACTERISTICS OF A HEALTHY CYBER ECOSYSTEM

These three factors call for the creation of a healthy *cyber ecosystem*. "Like natural ecosystems," noted a March 2011 white paper written by the US Department of Homeland Security (DHS), "the cyber ecosystem comprises a variety of diverse participants—private firms, non-profits, governments, individuals, processes, and cyber devices (computers, software, and communications technologies)—that interact for multiple purposes. Today in cyberspace, intelligent adversaries exploit vulnerabilities and create incidents that propagate at machine speeds to steal identities, resources, and advantage." As attackers constantly probe for the weakest link in a defense, "cyber devices [must] collaborate in near-real time."[6] In other words, they must be able to learn from their activities, creating and sharing that intelligence through collaborative community-driven initiatives such as Trusted Automated eXchange of Indicator Information (TAXII; https://taxii.mitre.org) and its Structured Threat Information eXpression (STIX; https://stix.mitre.org) language.

Motivated by concerns that cyberattacks are becoming "more frequent, more widespread, and more consequential," the DHS white paper outlined three essential building blocks of a healthy cyber ecosystem. First, automated mechanisms are needed to detect cyberattacks and intrusions and mitigate them at machine speeds. Second, semantic, technical, and policy interoperability among automated defense systems is essential to promote shared situational awareness and facilitate rapid machine-to-machine exchange of threat and incident data. The National Strategy for Trusted Identities in Cyberspace (www.nist.gov/nstic) describes technical and semantic interoperability as "the ability for different technologies to communicate and exchange data based upon well-defined and testable interface standards," while policy interoperability is "the ability for organizations to adopt common business policies and processes (e.g., liability, identity proofing, and vetting) related to the transmission, receipt, and acceptance of data between systems." Third, authentication is required to ensure that all parties participating in cyber defense, whether human or machine, are who they claim to be.

Since the white paper's release, two other necessary capabilities have been identified. First, individual cyber elements must be more resilient to attack and better able to maintain the integrity of their functionality and mission support through reduction of latent weaknesses that attackers could exploit. Second, mechanisms and infrastructure for machine-speed sharing of information must be developed. In this area, TAXII/STIX shows promise.[7]

TODAY'S CHALLENGES

Successfully protecting the IoT will require creation of a scalable and sustainable cyber ecosystem within the IoT that actively adjusts to and mitigates threats and malicious activities while being reliable, robust, and affordable. When fully established, the future cyber ecosystem will give people around the world the freedom to live, work, and play safely and securely in cyberspace, provided they take a few common-sense defensive precautions. Achieving this goal of a healthy cyber ecosystem requires addressing the following challenges: scalability, sustainability, affordability, resiliency, capability, interoperability, standards, automation, and adaptability.

Scalability, sustainability, and affordability

Today's cybersecurity processes fail to scale largely because they require too many professionals and experts to stay abreast of the latest vulnerabilities and required patches, monitor and analyze all manner of network activities, respond to alerts, understand what is happening at any given time, decide whether and how to respond, and implement response and recovery actions. Scalability demands that we automate the full spectrum of cybersecurity operations—sensing, sense-making, decision-making, and acting—to the greatest extent possible, shifting experts' role from being *in* the loop (in the critical path of all cyber-defense activities) to *on* the loop (monitoring and supervising largely automated defense and response functions). Not all cyberattacks can be addressed using automated processes, but moving from mostly human-speed processes to mostly orchestrated machine-speed processes would enable the powerful cadre of cyberprofessionals to concentrate their efforts on those classes of attacks that today are beyond the means of automated responses.

Scalability also demands that we make the individual elements of the cyber ecosystem more resilient to attack, with fewer inherent weaknesses and flaws for exploit by attackers. Today's cybersecurity processes associated with development, acquisition, and operations are unsustainable largely because the supporting commercial solutions often fail to integrate fully and effectively with one another, and/or are dependent upon costly, centralized government data feeds. To achieve scalability and sustainability, the cyber ecosystem will increasingly need to replace centrally managed government data feeds with federated commercial ones. Trusted and authoritative information providers must eventually prepare and disseminate most of the vital cybersecurity data in standardized machine-consumable formats.[7]

Sustainability and affordability demand that we proactively improve the security, resiliency, and effectiveness of our IoT by reducing the attack surface through supply-chain and software-quality improvements, thereby reducing cost; and by fostering technology innovation through the use of integrated, adaptive, interoperable tools and federated data feeds, which are based on a common data model and international standards provided by a vibrant commercial market.

Resiliency and capability

Within the cybersecurity community, there is a strengthening movement toward designing cyberspace systems to be resilient—to be able to withstand and rapidly "bounce back" from adverse events. Deborah Bodeau and Richard Graubart[8] define *cyber resiliency* as "the ability of a nation, organization, or mission or business process to anticipate, withstand, recover from, and evolve to improve capabilities in the face of adverse conditions, stresses, or attacks on the supporting cyber resources it needs to function." In addition to the long-term strategic goal of improving the overall quality, reliability, and integrity of software and ICT, there is a need to implement cyber resiliency engineering, a "sub-discipline of mission assurance engineering which considers (i) the ways in which an evolving set of resilience practices can be applied to improve cyber resiliency, and (ii) the trade-offs associated with different strategies for applying those practices."

Cybersecurity capabilities that effectively and efficiently protect the nation's IoT will emerge from the interactions of many discrete components, each contributing a needed function or service that is distributed across many heterogeneous devices and networks. These components need to contact and authenticate each other, establish secure communication channels, exchange data within defined access limits, and then use the data they have exchanged. To the extent that they do so successfully, the cybersecurity components of the cyber ecosystem are said to be interoperable and operate as an integrated set of capabilities.
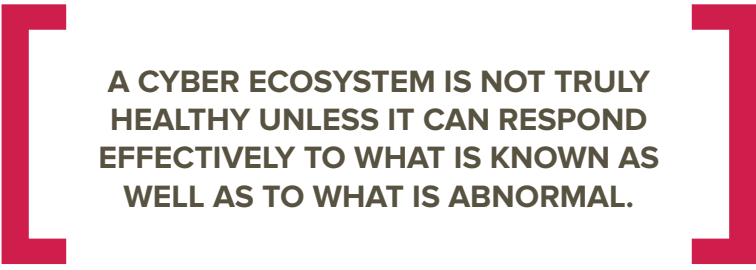
Interoperability, standards, automation, and adaptability

One way cybersecurity staff can achieve interoperability among disparate components is to acquire all products and services from a single vendor. While this may be beneficial in the short term, it could later lead to vendor lock-in—a situation in which the cost

of switching to a competing product becomes prohibitive, thus committing the consumer to the deployed solution even if a demonstrably more useful or functional alternative exists. Industry standards can help prevent certain forms of vendor lock-in. When a system of systems (like a cyber ecosystem) can be formed by integrating

[**A CYBER ECOSYSTEM IS NOT TRULY HEALTHY UNLESS IT CAN RESPOND EFFECTIVELY TO WHAT IS KNOWN AS WELL AS TO WHAT IS ABNORMAL.**]

functional components that conform to standard interfaces, communication protocols, and data formats, it becomes possible to relatively easily replace any individual component with a new one, without regard to vendor. (Industry standards offer other benefits as well; limiting dependence on proprietary solutions is just one of the most common motivations.)

However, standards are no panacea. Unless multiple vendors are competing vigorously on price, quality, and support to deliver standards-conformant products and services, industry standards by themselves offer little value to the consumer. There is no advantage to having freedom to choose without having meaningful choices. Fortunately, successful industry standards can and often do help create the conditions that sustain a vibrant market.

Today, automated cybersecurity defense depends on vast and growing volumes of human knowledge and insight distilled at high labor cost into

bundles of data that are formatted and structured for machine consumption, then disseminated over government-maintained channels. Significant government outlays over the years helped lay the foundation for a healthy cyber ecosystem, but such funding cannot continue indefinitely given current budget constraints. Moreover, central authorities, whether government-funded or not, cannot possibly keep up with the growing scope of automated cybersecurity defense content-development efforts.

A healthy cyber ecosystem must support adaptive responses to risks associated with both identified and suspected threats. As soon as a system vulnerability or pattern of malicious activity becomes known, trustworthy and actionable information needs to be broadly disseminated to all stakeholders—in standard formats, using common interfaces and secure communication protocols such as STIX and TAXII, with the requisite identity and access management controls—and then acted upon as soon as is practicable. Although this is much easier said than done, it is the best understood and most easily managed scenario in the entire cyber ecosystem.

Unfortunately, persistent and innovative phishing and social-engineering exploits, as well as the active underground market in zero-day attacks,

require cyber-ecosystem participants to be ever alert to the possibility that malicious external or insider attackers may have penetrated a network's defensive layers. Vigilance of this sort demands integrated, coordinated, and finely tuned capabilities using commonly understood concepts and terminology to accurately distinguish the ordinary from the anomalous, selectively increase scrutiny where warranted, actively test whether newly observed behavior is merely a novel manifestation of normal operations, and modify network settings to safely thwart malicious objectives without undermining operational missions or business functions. A cyber ecosystem is not truly healthy unless it can respond effectively to what is known as well as to what is abnormal and might indicate an attack or intrusion in progress.

THE FUTURE: INTEGRATED ADAPTIVE CYBER DEFENSE

Integrated Adaptive Cyber Defense (IACD) is the concept that commercial and government security solutions will be based on an open architecture for automated, adaptive, and dynamic cybersecurity assessment, mitigation, and defense at the enterprise, intra-enterprise, and inter-enterprise levels. This flexible, standards-based architecture, shown in Figure 3, will allow rapid insertion and integration of existing as well as future automated cyber-defense technologies and infrastructures. It must support automated messaging using a common data model and standardized exchange mechanisms, and be capable of applying agreed-upon rules to initiate actions within and across the collection of enterprises participating in the cyber ecosystem; that is, it must
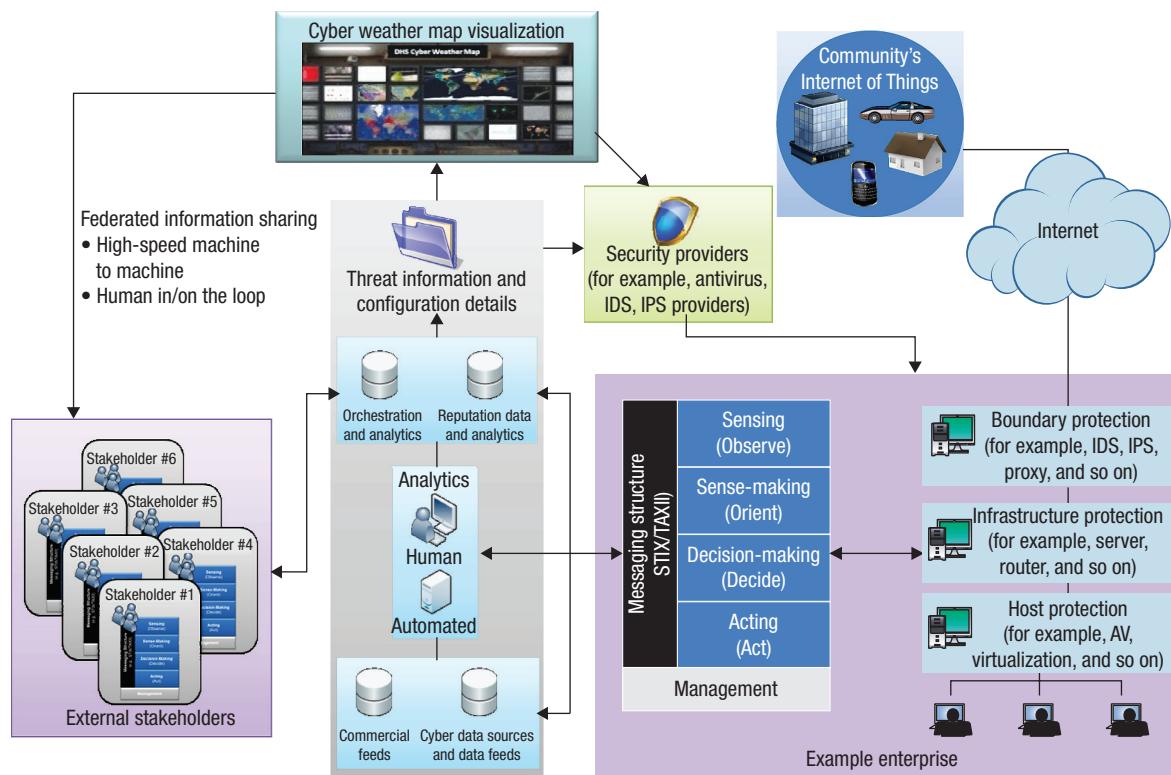
FIGURE 3. The flexible, standards–based Integrated Adaptive Cyber Defense (IACD) conceptual architecture will allow rapid insertion and integration of existing as well as future automated cyber–defense technologies and infrastructures.

support "whole enterprise" information exchange and action, as well as information exchange and action among semiautonomous business units and between enterprises. Message receivers must be able to identify and authenticate the source of each message, and to adjudicate whether a request for action can be performed automatically or only after review and approval by authorized parties.

Integrated capabilities include a communications medium with standard interfaces, message transport protocols, and message sets that support federated machine-speed exchange of cybersecurity information. Standard interfaces and common data syntax and semantics enable compatible components to connect to and interoperate through the communications medium. Standard protocols and data formats let components output and ingest data in a way that other standards-conformant components can understand. Standard message sets enable all connected components to communicate with one another among different enterprises. Messages must be tamper-resistant and include credentials that allow senders' identities and authorizations to be reliably determined. Components must be able to process and act on received messages within contextually determined time limits appropriate to the overarching cybersecurity objective. Depending on the context, cyber-relevant time could be nanoseconds, microseconds, seconds, minutes, or perhaps even hours.

Interoperable, modular commercial cybersecurity tools will provide integrated services across six logical functional areas:

› *Sensing* involves monitoring the cyber environment using devices or people to obtain snapshots of current operational states and risk exposures attributable to exploitable weaknesses in installed ICT/software. Sensing includes signature-, reputation-, and behavior-based capabilities.

› *Sense-making* involves applying rule sets, recognizing patterns, and using advanced algorithms to assess the dynamic cyber environment in many contexts. It is performed by interoperable tools, with or without human-on-the-loop review as dictated by circumstances. Sense-making takes advantage of federated information-sharing capabilities.

› *Decision-making* involves formulating candidate response actions that empower enterprise decision-makers to evaluate alternatives and select the best course of action (COA). Decisions are made by automated tools, with human-on-the-loop review as dictated by circumstances. Decision-making selects among available response actions, while leaving the action decision itself

with the cyber asset owner.

› *Acting* involves implementing selected COAs in cyber-relevant time. Preventative and response COAs should be executed automatically to the greatest extent possible, with automated detection and identification of

into the current security state of their networks as well as other networks on which their businesses or missions depend. The insight offered by a common operational picture (COP) lets operators properly understand why automated COAs are being

human-originated actions and the enabling and blocking of them based on an analysis of the sender or source reputation and object history is an aspect of IACD functionality.

Centralized, enhanced situational awareness will help human operators perceive and evaluate security activities and trends, provide a "weather map" of looming "cyberstorms," and reveal the susceptibility of an organization's ICT/software to specific threats and malware. Current technologies such as big data analytics, reputation-based scoring, visualization, presentation, and dissemination are limited; cooperative action is needed to promote and guide development of new capabilities that can eventually be incorporated into the cyber ecosystem. A federated ability to integrate, analyze, and disseminate information in milliseconds is needed.

> **ESTABLISHING THE IACD ARCHITECTURE WILL BE A COMPLEX AND TECHNICALLY DEMANDING ACTIVITY CARRIED OUT INCREMENTALLY.**

patterns of attacks and correlation to known weaknesses and vulnerabilities in ICT/software with appropriate machine-speed mitigations. Human operators should be notified and given situational awareness of executing COAs, but the operators should be involved in the process only when needed to ensure that automated actions are properly authorized and to manage any impacts on critical business or mission functions. As this is an immature area requiring more research, the only COAs that will be used initially are those with well-understood impacts, such as sending an automated email or adding a firewall block.

› *Federated information-sharing* (shared situational awareness and shared analysis) of cybersecurity data—not only within but also among disparate enterprises—is a critical enabler of automated COAs. Human operators need accurate insight

recommended or invoked to protect ICT/software-enabled systems with latent weaknesses and vulnerabilities from detected or suspected exploits or attacks, and helps them coordinate responses with peers who may be coping with the same or similar security conditions.

› *Management functions* allow operators to view data such as packet streams, alerts, and reports, and to select actions in which organizational policy requires human approval. They also provide automated workflow and overall control of capabilities and tools that support and perform cybersecurity functions while ensuring privacy of personal information. This automated workflow is applicable to all actions on a risk-assessed basis, from clicking on a URL to opening an email attachment. Cyber risk assessment is commonly referred to as reputation scoring. Orchestration of

The IACD architecture will make use of an array of technical standards to ensure component interoperability and openness to any conformant automated cyber-defense product or service with a common set of foundational concepts about what is being exchanged. Standards must be designed with the consensus of government, industry, and the general public to ensure widespread adoption. The goal is for all security customers to use IACD to either implement their own solutions or purchase a turnkey service from a vendor.

Establishing the architecture will be a complex and technically demanding activity carried out incrementally. Each step will yield new lessons, and must be guided by insights gained from smaller-scale, lower-risk, and more narrowly focused research and

experimentation. Demonstration prototypes, technology assessments, and capability pilots will be needed to evaluate operational concepts and to attract and inspire stakeholders. As the market will not be idle while this takes place, commercial solutions must be tested and evaluated with a goal of understanding where and how they could be incorporated into the emerging cyber ecosystem. Lastly, because the architecture supports a vision of automated adaptive cyber-defense capabilities well beyond the state of the art, investments in advanced research will be needed to explore and extend the art of the possible.

The above envisaged IACD capabilities will help achieve a secure cyber ecosystem but will require a substantial commitment of resources and the coordination of government, academia, and international and industry partners over many years. Four goals critical to cyber resiliency that are the most feasible to accomplish over the next 5 to 10 years are the development of a standards-based architecture that supports rapid technology insertion, capabilities for automated COAs, a weather-map capability with federated data feeds, and trusted information-sharing at machine speeds using common terminology and foundational concepts. However, such efforts will come to naught without a persistent focus on affordability, risk reduction, scalability, effectiveness, and efficiency.

Increased use of automation offers the greatest prospect of containing costs and reducing risks, but automation is no silver bullet—it depends on our ability to distill expert human knowledge and skill in cybersecurity sensing,

sense-making, decision-making, information sharing and analytics, and acting into forms amenable to manipulation and execution by machines. As the cyber ecosystem's IACD emerges and evolves, care must be taken at all times to avoid simply creating a different set of comparable (or worse) costs and risks.

Scalability, effectiveness, and efficiency are also key considerations. IACD's various implementations must be scalable to fit the needs of small as well as large organizations; be more effective than current methods in anticipating, preventing, disrupting, and countering attacks and intrusions; and make more efficient use of human and machine resources while protecting privacy. Demonstrating this will require new metrics for quantifying and evaluating the costs and benefits of alternative cybersecurity solutions. The overall principle is to enable all Internet technologies to play a role in protecting traffic and IoT components. We must do with numbers and data correlation what biology does with chemicals to create a dynamic immune system with automated detection and response. We must optimize the use of humans on the loop for complex or politically driven incidents that cannot

be addressed by automation and for "antibiotic-resistant" intrusions that can result from the use of automation against common attacks.

Our efforts to evolve the cyber ecosystem must result in solutions that promote adaptability and agility of response. As the tactics, techniques, and procedures of cyber adversaries continuously adapt and evolve, so too must the cybersecurity defense mechanisms and methods implemented within the cyber ecosystem driven by IACD. ☐

ABOUT THE AUTHORS

PETER FONASH is CTO for the Office of Cybersecurity and Communications in the National Protection and Programs Directorate (NPPD) within the US Department of Homeland Security (DHS). He is also an adjunct faculty member of the University of Tulsa's College of Engineering and Natural Sciences and an advisory board member of George Mason University's Volgenau School of Engineering. Fonash received an MS in engineering from the University of Pennsylvania, an MBA from the University of Pennsylvania Wharton School, and a PhD in information technology and engineering from George Mason University. He is a member of IEEE. Contact him at peter.fonash@hq.dhs.gov.

PHYLLIS SCHNECK is the Deputy Under Secretary for Cybersecurity and Communications in the NPPD and the DHS's chief cybersecurity official. A pioneer in the field of information security and security-based high-performance computing with seven information-security patents, she received an MS and BS in computer science from Johns Hopkins University and a PhD in computer science from Georgia Tech. Contact her at phyllis.schneck@hq.dhs.gov.

REFERENCES

1. C.R. Schoenberger, "The Internet of Things," *Forbes*, 18 March 2002; www.forbes.com/global/2002/0318/092.html.
2. D. Evans, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, white paper, Cisco, Apr. 2011; www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
3. D. Needle, "Wi-Fi Pacemaker Monitors Patient via the Web," *InternetNews*, 9 Aug. 2009; www.internetnews.com/breakingnews/article.php/3834011/WiFi

+Pacemaker+Monitors+Patient+Via+the+Web.htm.
4. E.A. Corriveau et al., "Effect of Carelink, an Internet-Based Insulin Pump Monitoring System, on Glycemic Control in Rural and Urban Children with Type 1 Diabetes Mellitus," *Pediatric Diabetes*, vol. 9, no. 4, 2008, pp. 360–366.
5. "Warning—Medical Devices May Be Subject to Cyber Attacks," *i–HLS*, 5 July 2013; http://i-hls.com/2013/07/warning-medical-devices-may-be-subject-to-cyber-attacks.
6. *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*, white paper, US Dept. of Homeland Security, 23 Mar. 2011; www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.
7. S. Barnum, *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX)*, white paper, MITRE, 20 Feb. 2014; https://stix.mitre.org/about/documents/STIX_Whitepaper_v1.1.pdf.
8. D.J. Bodeau and R. Graubart, *Cyber Resiliency Engineering Framework*, tech. report MTR 110237, MITRE, Sept. 2011; www.mitre.org/sites/default/files/pdf/11_4436.pdf.

Selected CS articles and columns are also available for free at **http://ComputingNow.computer.org**.